HealthEquity
Building Health Savings

Dear County Of Yuma,

Please be aware that we have identified an increase in phishing and fraud attempts with HealthEquity member accounts. After the identification of activity patterns, we are confident that HealthEquity's systems have **not** been breached. However, we have determined that fraudsters are obtaining personal information from other illicit sources to compromise accounts. HealthEquity is dedicated to increased security and monitoring account activity. Below is important information and relevant resources.

Increased phishing and fraud attempts
Along with other financial accounts, fraudsters recognize the growing value of health savings accounts (HSAs) and are increasingly targeting them industrywide. We encourage members to protect HSAs as they would any other bank account.

HealthEquity security enhancements
In response to increased fraudulent attempts, HealthEquity has enhanced information security in the following ways:

The last four digits of the debit card associated with an account are now required for first time log in. Debit cards are only accessible to members via mail.
Captcha authentication is required when logging in to the member portal for the first time and after any failed password attempts.
Callers will be asked additional verification questions when contacting member or employer services.
Continual monitoring and blocking of malicious IP addresses.
Ongoing collaboration with the FBI and third-party forensics team.
Educational campaign for members to combat phishing and fraud. Emails will be sent to members to promote our Tackle Phishing and Fraud resource site (see below).

Reject "phish" bait
We recommend sharing the following tips with your employees and have included the email template below for your convenience:

Log into your account: As soon as your account is open, log in and create a unique and secure password. Do not use the same password for multiple sites.
Change your password frequently: We recommend changing passwords every 90 days.
Don't click on email links: Manually type in the website that you know is correct.
Learn to identify suspicious details: Understand what to look for to uncover an email scam. Details are outlined at HealthEquity.com/protect.
Look for secure site indicators: Authentic login sites have certificates of security

indicated by a locked keypad icon by most browsers or an "s" added to the URL.
Review transaction history frequently.

Report fraud
If you feel you or your employees have received an email from a scammer posing as HealthEquity:

Forward the entire email to phishing@healthequity.com.
If links were clicked or sensitive HealthEquity information was provided to a suspected scammer, call member services immediately at 866.346.5800.
Report the email to the Federal Trade Commission by forwarding it to spam@uce.gov.

Resources
The following resources provide additional education and information:

Tackle Phishing and Fraud website (HealthEquity.com/protect or accessible from our homepage).
An email template to communicate tips to employees is included below.
A list of frequently asked questions is included below.

As always, we are here for support and appreciate your continued partnership. If you have further questions, please contact us at employerservices@healthequity.com.

HealthEquity Employer Services

Frequently asked questions

Introduction
HealthEquity has seen an increase in phishing and fraud attempts on HSAs. Fraudsters recognize the growing value of HSAs and are targeting them industrywide, much like they have with banking institutions. The following FAQs are an educational resource to our valued partners to help prevent further incidents.

Situational overview

Have HealthEquity's systems been breached?
No, we are confident that HealthEquity's systems have not been compromised.

How are you sure that HealthEquity hasn't been breached?
There are several indicators that make it evident that a breach has not occurred:

1. Fraudsters continue to use phishing tactics in an attempt to steal account login credentials. This is evidence that they do not have login information or access to accounts.
2. Phishing emails are being sent to entire organizations, and target individuals who don't even have an HSA.
3. The limited success rate of account takeover.
4. Fraudsters have resorted to credential stuffing as a strategy to use stolen or purchased credentials from other sources and accounts to attempt hijacking.

5. Based on our own monitoring and an ongoing review by a third-party forensic team, we are highly confident that a system breach has not occurred.

What fraudulent activity has been occurring?
We have seen a few trends:

1. First time account activation: Because members are able to access their funds with a provided debit card, many do not log into the member portal to establish a secure username and password. Authentication of new accounts requires information such as name, social security number and date of birth. This information is increasingly available to fraudsters on the black market and as a result of breaches elsewhere. Fraudsters are using this information to initiate a first time login and hijack accounts.
2. Phishing: Fraudsters are posing as HealthEquity to send emails to employees of HealthEquity clients. Because fraudsters don't know which employees have an HSA, they send emails to all, or a large number of employees. The emails are urgent in nature and request immediate verification of account information. Users are urged to click on a link to log into their account. When the link is clicked, users are directed to a website that looks like the HealthEquity login page, but is actually a spoofed page created by fraudsters. When credentials are input, the fraudsters are given access to the account.
3. Credential stuffing: Fraudsters acquire "spilled" credentials obtained from various illicit sources. These credentials are then tried at various other sites, including HealthEquity, to gain account access. Individuals who use the same username and passwords on various sites are particularly vulnerable to this technique.
4. Vishing: Fraudsters have contacted HealthEquity member services, armed with personal information accessed from other illicit sources, trying to reset the password to accounts or initiate money transfers.
5. EFT (electronic funds transfer) fraud: Once an account has been taken over using one of the methods above, the fraudster attempts to transfer funds out of the account.

HealthEquity mitigations

What is HealthEquity doing to protect against fraud?
We are implementing several new defenses to combat the recent fraud attempts:

1. When logging into an account for the first time, members are now required to provide the last 4 digits of the debit card associated with an account. Because cards are only mailed to home addresses submitted by employers, fraudsters don't have access to these digits. (Completed)
2. Captcha authentication is required when logging in to the member portal for the first time and after any failed password attempts. This reduces the likelihood that automated robot authentication attempts will be successful. (Completed)
3. Active monitoring and blocking of malicious IP addresses. (Ongoing)
4. Callers are asked additional verification questions when contacting member or employer services. (Completed)
5. Sender policy framework (SPF) has been implemented. This email validation system detects email spoofing by providing a mechanism allowing receiving mail exchanges to verify that incoming email from our domain comes from an authorized host.
6. We continually initiate take downs of phishing sites. (Ongoing)

7. Additional authentication and EFT controls will be implemented. (Coming weeks)
8. An educational campaign, Tackle Phishing and Fraud, is being launched to educate members on how to protect their accounts. A website with various resources has been established (HealthEquity.com/protect) and is accessible from our homepage. Emails with tips and tricks will be sent to members. (Ongoing)

What is HealthEquity doing to monitor fraud attempts?
We have an entire team dedicated to analyzing data and patterns. They use a multipronged approach to monitor geographical, IP, transactional and EFT activities. In a large majority of cases, we are able to identify fraud attempts before damage is done. We have hired a third-party data forensics team to review our processes to make sure we are doing all that we can to protect our members.

Employer defenses

What can employers do to help fight fraud?
There are several ways you can help your employees:

1. Encourage your employees to treat their HSAs like any other banking account and safeguard login credentials. Support HealthEquity's Tackle Phishing and Fraud campaign and spread the word.
2. Log into the HealthEquity employer portal to view a current list of known phishing IP addresses and domains that you can block.
3. Enable sender policy framework (SPF) in hard fail mode so that your system can determine if e-mails that appear to be from HealthEquity are sent from authorized HealthEquity e-mail servers.

Member defenses

What can members do to protect their accounts?
Here are a few things members should do to help reject "phish" bait:

1. **Log into your account:** As soon as your account is open, log in and create a unique and secure password.
2. **Don't use the same password for multiple sites.** If one account is compromised, fraudsters may attempt the combination of credentials on other sites.
3. **Change your password frequently:** We recommend changing your password every 90 days.
4. **Don't click on email links:** If you are asked to urgently sign into your account, type in the website yourself that you know is correct. HealthEquity.com is our official site where you can access the secure login page.
5. **Learn to identify "phishy" details**: Understand what to look for to uncover an email scam. Here are some common giveaways:
   - Subject line is "Urgent" or "Immediate Action"
   - Sender name looks odd or unfamiliar
   - Dear Customer... The greeting is not personalized with your name
   - Please confirm your identity... Legitimate sites won't ask to verify identity
   - Misspellings and grammatical errors, including UK spellings
   - Attachments: Unless you requested a document from HealthEquity to be sent via email
   - Links that look modified or unusual (healthequ1ty.com or the link may not - contain

healthequity)
    - Vague information
    - Asking for information, such as the last 4 of your HealthEquity debit card
6. **Look for secure site indicators:** Authentic login sites have certificates of security indicated by a locked keypad icon by most browsers or an "s" added to the url, i.e. https://www...
7. **Enable email notifications** to alert you when information has changed on your account
8. **Review your transaction history frequently**
9. When in doubt, **call HealthEquity** 24/7 at the number found on the back of your debit card or 866.346.5800.

For victims of phishing and fraud

What do I do if I receive a phishing email?
Forward the entire email to phishing@healthequity.com, then delete the email completely. Do not click on any links. You can also report the email to the Federal Trade Commission by forwarding it to spam@uce.gov.

What do I do if I click a suspicious link or provide credentials to a suspicious site?
Call HealthEquity member services immediately. We are available 24 hours a day and can be reached at the number on the back of your debit card or 866.346.5800.

What happens if my funds are lost due to fraud?
HealthEquity will evaluate your situation and determine how to proceed. If HealthEquity approves restoring your lost funds, we require a few steps:

1. Call HealthEquity to report the fraud and open case number
2. Sign and notarize release form and liability waiver
3. We also recommend that victims file a police report with local law enforcement and provide the case number and detective's contact information.

Once these steps are completed and approved, HealthEquity will deposit your lost funds into your account within 10 business days.

Are my funds insured by FDIC?
Yes, HSAs are FDIC-insured. However, FDIC insurance does not cover fraudulent activity. It only protects your funds in the event that your financial institution goes out of business.

If my account is compromised, what other information is at risk?
Fraudsters who compromise an account have access to other personal and financial information that is associated with the account.

Is HealthEquity legally required to notify members if their account has been compromised?
The legal requirement to notify members with compromised accounts varies from state to state. Where required, we comply and communicate to members. In every case, we evaluate any information that might have been accessed and the risks associated with each situation and provide notification as warranted.

Will HealthEquity provide credit monitoring if my account is compromised?
We offer free credit monitoring services to compromised accounts on a case-by-case basis based on the facts of each incident.

Email template to communicate tips to your employees:

Dear [Employee Name],

HealthEquity has made us aware of increased phishing scams where fraudsters pose as HealthEquity in an attempt to steal login credentials to health savings accounts (HSAs). Below are tips to help stop fraudsters and protect your assets.

What is phishing?
Phishing is an attempt to obtain sensitive account information such as a username or password by posing as a legitimate company, mainly through email.

How to spot a phishing email
Here are some common giveaways:

Subject line is "Urgent" or "Immediate Action"
Sender name looks odd or unfamiliar
Dear Customer… The greeting is not personalized with your name
Please confirm your identity... Legitimate sites won't ask to verify identity
Misspellings and grammatical errors, including UK spellings
Attachments: Unless you requested a document from HealthEquity to be sent via email
Links that look modified or unusual (healthequ1ty.com or the link may not contain healthequity)
Vague information

HealthEquity will never ask you for your SSN, PIN, card number or any personal information via email, text, phone/recorded audio, or through social media. They may ask for your SSN and other personal information to verify they are speaking to you when you call.

Protect your information
Here are a few things that you can do to help reject "phish" bait:

Log into your account: As soon as your account is open, log in and create a unique and secure password. Do not use the same password for multiple sites.
Change your password frequently: We recommend changing passwords every 90 days.
Don't click on email links: Manually type in the website that you know is correct.
Learn to identify suspicious details: Understand what to look for to uncover an email scam. Details outlined at HealthEquity.com/protect.
Look for secure site indicators: Authentic login sites have certificates of security indicated by a locked keypad icon by most browsers or an "s" added to the URL.
Review transaction history frequently.
Enable email notifications to alert you when information has changed on your account

When in doubt, **call HealthEquity** 24/7 at 866.346.5800.

HealthEquity also continues to evaluate and implement additional anti-spoofing measures to keep your account safe and secure.

Remember, you are the first line of defense as phishing attacks become more frequent. If you need help logging in or believe you may have provided your credentials to someone else, please contact HealthEquity at 866.346.5800. They are available every hour of every day to assist you.

[Insert signature]

HealthEquity is located at 15 W. Scenic Pointe Dr., Draper, UT 84020